REMARKS

The above amendment and these remarks are responsive to the Office action of Examiner Thong H. Vu, mailed 16 July 2004.

Claims 1-24 are in the case, none as yet allowed.

35 U.S.C. 101

Claims 1-7, 9-10, 12-14, 16-20, 22-23 have been rejected under 35 U.S.C. 101 because the disclosed invention is inoperative and therefore lacks utility. The reason provided by the Examiner is that "the double nested [concept] is not described in the specification."

Applicants traverse.

The "double nested" concept is adequately described.

The abstract refers to double nesting as follows:

"A communication network includes a plurality of nodes, selectively including a client, a remote gateway Internet service provider, the Internet, a local enterprise gateway, and an enterprise internal network. A local coincident endpoint is established at a first node for an outer connection with a remote node and an inner connection with a different remote node. The nodes participate in negotiations on the outer connection to set up the inner connection as a secure connection. Thereafter, responsive to communications on the inner connection, the first node establishes links to the outer connection selectively to receive or send communications double nested on the outer connection."

Reference is also made to the phrase "double nest[ed, ing]" or "doubly nested" at page 5, line 18, page 18, lines 15 and 19, and in several of the claims - all of which is considered part of the original specification as filed.

Figures 2, 3, 4 and 5 all show aspects of the invention which are pertinent to and describe this concept of double nesting. The text describes the figures and the concept of double nesting as it relates to the present invention.

In connection with Figure 2, the specification at page 7, line 2 to page 9, line 12, describes three scenarios B, C, and D.

In connection with Figure 4, the specification at page 11, line 10 to page 12, line 13, describes the organization of the nested connection table and how it is used.

In connection with Figure 3, the specification at page 12, line 14 to page 15, line 7 explain the steps in setting up the double nested connection at the coincident endpoint.

In connection with Figure 5, the specification at page 15, line 8 to page 19, line 6 shows the logical structure of the TCP/IP packets as they flow back and forth between the remote endpoint and the coincident endpoint (enterprise gateway).

Important steps of the process which result in the creation of a double nested connection, steps 80 and 82, are described on page 18, line 10, to page 19, line 3, which states:

"In step 80, gateway 16 recognizes that the starting

VPN connection t2 is the result of prior tunneled IKE traffic from inside connection t1 24.

"In step 82, code in the kernel of gateway 16 links the SA for this new, inner connection t2 26 to the proper SA for the outer connection t1 24 so that traffic is doubly nested. Thus, [local coincident endpoint] LCE 40 is created.

"As a result of creating LCE 40, traffic outbound from network 18 is first put by gateway 16 in inner connection t2 26, then in outer connection t1 24 and sent doubly nested on to client 10. At ISP 12, the outer connection t1 24 is removed, and traffic continues on inner tunnel t2 26 to client 10, where it is decapsulated." (Emphasis added).

All of this taken together clearly describes to one of ordinary skill in the art the concept of "double nested" in sufficient detail to make and use the present invention, and provides specification support for this concept in the claims.

Applicants request that the Examiner reconsider and

withdraw the rejection of claims 1-7, 9-10, 12-14, 16-20, 22-23 under 35 U.S.C. 101.

35 U.S.C. 102

Claims 8, 11, 21, and 24 have been rejected under 35 U.S.C. 102(e) as anticipated by Ylonen et al. (Ylonen, 6,438,612 B1).

Applicants traverse, and argue that the Examiner has not made the required prima facie case of anticipation, which requires that the Examiner provides

1. a single reference
2. that teaches or enables
3. each of the claimed elements (arranged as in the claim)
4. expressly or inherently
5. as interpreted by one of ordinary skill in the art.

With respect to claim 11, the cited references in Ylonen do not contain the words or describe the concepts

stated in the Office Action. For example, concepts in claim 11 which are missing from Ylonen include the following:

a. "start an outer connection"

b. "establish a secure nested inner connection"

c. "over said outer connection parameters defining said secure nested inner connection"

d. "operating said client node to start said inner connection"

e. "start said inner connection"

f. "operating said gateway node to recognize the start of the said inner connection and to link said inner connection to said outer connection"

Yes, both Ylonen and applicants' invention relates to virtual private networks (VPNs).

However, Ylonen nowhere discusses or describes nest, nested, nesting, coincident, or coincident endpoint. In addition, the concepts of nested VPN connections expressed in other words to not appear in Ylonen. Ylonen does not related to nested VPN connections, and does not describe nested VPN connections with coincident endpoints. Therefore, the prima facie case for anticipation of claim 11

has not been established by the Examiner's citation of Ylonen.

With respect to claim 8, again, the cited references in Ylonen to not even mention "outer connection", "coincident endpoint inner connection" nor are these claimed concepts otherwise described.

With respect to claims 21 and 24, yes, both Ylonen and applicants' invention use VPN and security associations. These are not what is claimed in claims 21 or 24. The cited references in Ylonen do not mention or otherwise describe "outer connection" or "coincident endpoint inner connection" as claimed.

Applicants set forth below independent claims 8, 11, 21 and 24, highlighted to show certain distinctions with respect to Ylonen.

8. A method for operating a first one of a plurality of nodes in a communications network, comprising the steps of:

establishing at said first node a coincident endpoint for an outer connection and an inner connection with at

least one second node in said network;

responsive to starting communication of traffic over said connections, establishing a link from said inner connection to said outer connection; and

responsive to said links, selectively encapsulating said traffic to said outer connection for transfer to said second node or decapsulating said traffic from said outer connection for receipt at said first node.

11. Method for nesting connections between a plurality of nodes in a communication network, said nodes including a client, and internet service provider (ISP), an enterprise gateway, and an internal network, comprising the steps of:

operating said client node to call said ISP node;

operating said ISP node to start an outer connection with respect to said gateway node and to return an IP address to said client node;

operating said client node to send to said gateway node over said outer connection a request to establish a

secure nested inner connection;

operating said client node and said gateway node to negotiate over said outer connection parameters defining said secure nested inner connection, and saving said parameters at said gateway node; and thereafter

operating said client node to start said inner connection; and

operating said gateway node to recognize the start of said inner connection and to link said inner connection to said outer connection.

21. A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for operating a first one of a plurality of nodes in a communications network, comprising the steps of:

establishing at said first node a coincident endpoint for an outer connection and an inner connection with at least one second node in said network;

responsive to starting communication of traffic over said connections, establishing a link from said inner connection to said outer connection; and

responsive to said links, selectively encapsulating said traffic to said outer connection for transfer to said second node or decapsulating said traffic from said outer connection for receipt at said first node.

24. A computer program product or computer program element for operating a first one of a plurality of nodes in a communications network according to method steps comprising:

establishing at said first node a coincident endpoint for an outer connection and an inner connection with at least one second node in said network;

responsive to starting communication of traffic over said connections, establishing a link from said inner connection to said outer connection; and

responsive to said links, selectively encapsulating said traffic to said outer connection for transfer to said second node or decapsulating said traffic from

said outer connection for receipt at said first node.

The Examiner has not, consequently, made a prima facie case of anticipation. Applicants request that the rejection of claims 8, 11, 21, and 24 under 35 U.S.C. 102 be reconsidered and withdrawn.

35 U.S.C. 103

Claims 1-7, 9-10, 12-14, 16-20, 22-23 have been rejected under 35 U.S.C. 103 over Ylonen in view of Rao et al. (Rao, 6,674,756 B1).

Applicants traverse, and argue that the Examiner has not established a prima facie case of obviousness, which requires that the Examiner provides

1. one or more references
2. that were available to the inventor and
3. that teach
4. a suggestion to combine or modify the references,

5. the combination or modification of which would appear to be sufficient to have made the claimed invention obvious to one of ordinary skill in the art.

Applicants agree that the current application, Rao, and Ylonen all involve VPNs. Rao and Ylenen deal with the concept of "virtual routers", a concept which is not the subject of the current application. For example, Rao (column 2, lines 19-40) describes a switch partitioned into multiple virtual routers. However, Rao does not describe the following concepts: "nest", "nested", "nesting", "coincident", "coincident endpoint", "inner", or "outer". In addition, the concepts of nested VPN connections expressed in these or other words does not appear in Rao.

Therefore, the combination of Ylonen (which does not contain these concepts as previously discussed) and Rao (which does not contain these concepts) do not teach applicants claims.

Applicants independent claims are set forth below, underlined to highlight this concept of coincident endpoint which is entirely absent from both Rao and Ylonen.

1. Method for nesting connections between a plurality of nodes in a communication network, comprising the steps of:

receiving at a first node on an outer connection a request from a second node to establish a coincident endpoint for nesting an inner connection within said outer connection;

negotiating over said outer connection parameters defining said inner connection; and thereafter

responsive to communication occurring on said inner connection, at said first node linking to said outer connection for selectively receiving or sending said communication double nested on said outer connection.

5. Method for operating an enterprise gateway, comprising the steps of:

receiving at said gateway from a remote client a request to establish an outer connection;

receiving at said gateway over said outer connection a

request to establish, and thereupon negotiating parameters establishing, a secure inner connection;

responsive to outbound or inbound traffic on said inner connection, establishing links to said outer connection for communicating said traffic double nested on said outer connection.

15. System for nesting connections between a plurality of nodes in a communication network, comprising:

a first node on an outer connection for receiving a request from a second node to establish a coincident endpoint for nesting an inner connection within said outer connection;

said first and second nodes negotiating over said outer connection parameters defining said inner connection; and thereafter

said first node being responsive to communication occurring on said inner connection for linking to said

outer connection for selectively receiving or sending said communication double nested on said outer connection.

19. A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for nesting connections between a plurality of nodes in a communication network, said method steps comprising:

receiving at a first node on an outer connection a request from a second node to establish a coincident endpoint for nesting an inner connection within said outer connection;

negotiating over said outer connection parameters defining said inner connection; and thereafter

responsive to communication occurring on said inner connection, at said first node linking to said outer connection for selectively receiving or sending said communication double nested on said outer connection.

20. A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine to perform method steps for operating an enterprise gateway, said method steps comprising:

receiving at said gateway from a remote client a request to establish an outer connection;

receiving at said gateway over said outer connection a request to establish, and thereupon negotiating parameters establishing, a secure inner connection;

responsive to outbound or inbound traffic on said inner connection, establishing links to said outer connection for communicating said traffic double nested on said outer connection.

22. A computer program product or computer program element for nesting connections between a plurality of nodes in a communication network according to steps comprising:

receiving at a first node on an outer connection a

request from a second node to establish a coincident endpoint for nesting an inner connection within said outer connection;

negotiating over said outer connection parameters defining said inner connection; and thereafter

responsive to communication occurring on said inner connection, at said first node linking to said outer connection for selectively receiving or sending said communication double nested on said outer connection.

23. A computer program product or computer program element for perform method steps for operating an enterprise gateway according to method steps comprising:

receiving at said gateway from a remote client a request to establish an outer connection;

receiving at said gateway over said outer connection a request to establish, and thereupon negotiating parameters establishing, a secure inner connection;

responsive to outbound or inbound traffic on said inner connection, establishing links to said outer connection for communicating said traffic double nested on said outer connection.

Applicants assert that the Examiner has not made the required prima facie case of obviousness, and urges that claims 1-7, 9-10, 12-14, 16-20, 22-23 be allowed.

SUMMARY AND CONCLUSION

Applicants urge that the above amendments be entered and the case passed to issue with claims 1-24.

The Application is believed to be in condition for allowance and such action by the Examiner is urged. Should differences remain, however, which do not place one/more of the remaining claims in condition for allowance, the Examiner is requested to phone the undersigned at the number provided below for the purpose of providing constructive

assistance and suggestions in accordance with M.P.E.P. Sections 707.02(j) and 707.03 in order that allowable claims can be presented, thereby placing the Application in condition for allowance without further proceedings being necessary.

Sincerely,

E. B. Boden, et al.

By

Shelley M Beckstrand
Reg. No. 24,886

Date: 15 Oct 2004

Shelley M Beckstrand, P.C.
Attorney at Law
61 Glenmont Road
Woodlawn, VA 24381

Phone: (276) 238-1972